Audit Committee Leadership Network

April 2019

ACLN

VIEWPOINTS

Board oversight of privacy

Companies enjoy a wealth of opportunities to capitalize on the data they obtain from customers, employees, and business partners. They are using data analysis techniques to improve risk management, operating efficiency, customer relations, and product innovation. But in trying to capitalize on the data they are collecting, companies also face mounting public concerns over privacy, as reflected in new regulations and in heated debates on the use of personal data.

Privacy and data governance are becoming critical issues for a growing number of companies. Security is an important element, because data privacy requires data security. But the issue extends well beyond the need to protect data from unauthorized disclosure. New regulations and shifting consumer expectations are also altering the terms for the collection, storage, and use of personal data. In response, companies are reviewing their practices, and boards are ramping up their oversight.

On March 27, 2019, members of the Audit Committee Leadership Network (ACLN) discussed practices for enhancing data privacy oversight. They were joined for this discussion by Phil Nemmers, an Ernst & Young LLP partner knowledgeable in data protection and privacy issues, and by several executives responsible for privacy at their companies: Eduardo Andrade, global compliance and ethics officer at Booking Holdings; Harvey Jang, senior director, global data protection & privacy counsel at Cisco; and Tom Moore, chief privacy officer at AT&T. *For guest biographies, please see Appendix 1, on page 10. For a complete list of participants, please see Appendix 2, on page 13.*

Executive summary

ACLN members and their guests touched on several topics during their discussions before and during the meeting:[1]

- **Emerging constraints on data use** *(page 2)*

  Companies face increasing tensions between the opportunities to utilize data and the pressures to protect personal privacy. There has been considerable debate about this issue in recent years. New legal requirements have emerged, making privacy protection an important compliance imperative. At the same time, the issue goes beyond compliance to include the less explicit, but still significant, considerations associated with safeguarding a company's reputation and trustworthiness in the eyes of customers, employees, and the public.

tapestry NETWORKS

EY Building a better working world

- **The response from companies** *(page 4)*

  Achieving the right balance between providing adequate privacy protection and making productive use of personal data presents major challenges for companies. ACLN members and guests touched on the need for both centralized leadership and broad involvement of many functions—including business units—in the effort. They also discussed the specific challenges of obtaining informed consent for the use of personal data and deciding on appropriate disclosures in the event of a privacy violation.

- **Board oversight** *(page 7)*

  While the full board is ultimately responsible for oversight of privacy, ACLN members reported that several committees may be involved or take the lead, including the audit, compliance, and risk committees. Frequency and intensity of discussions about privacy still vary among boards; some boards raise the issue at every meeting, while others approach it on an ad hoc basis. The guests suggested that internal audit can help inform the board about the privacy control framework, and they advised ACLN members to ensure that their privacy function has sufficient resources and expertise.

For a list of discussion questions, see Appendix 3 on page 14.

Emerging constraints on data use

Companies are facing increasing tensions between effectively utilizing collected data and the ethical and regulatory limitations over its use. On the one hand, the proliferation of collected data and the emergence of new analytic tools are creating new opportunities for companies to improve their business. On the other hand, customers, employees, and other stakeholders may have concerns about how their data is collected and used. In recent years, debate has intensified in many quarters. This has led policymakers to impose significant conditions on how companies store, use, and share data. It has also raised awareness among the public at large, heightening the reputational issues involved.

Regulatory challenges

New laws and regulations are in force or in the works in several jurisdictions, and experts believe others will follow suit. The European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016, and it came into effect in May 2018. This regulation establishes new consumer rights and organizational responsibilities, including requirements like easily understandable requests for consent, transparency regarding how personal data is used, the right to have personal data erased, and the obligation for some organizations to appoint a data protection officer.[2]

In the United States, the Federal Trade Commission (FTC) has responsibility for enforcing fair trade practices in privacy and data use, and different federal laws and regulations govern the use of certain data. In financial services, for example, the Financial Services Modernization Act

(the 1999 Gramm-Leach-Bliley Act, or GLBA) regulates the collection and use of financial information and limits its disclosure—in some cases requiring institutions to disclose their privacy practices and allow consumers to opt out of sharing information.[3] Another example is the Health Insurance Portability and Accountability Act, which has provisions for protecting medical information.

While a law like the GDPR does not exist in the United States at the federal level, states are beginning to act. In June 2018, for example, California passed the California Consumer Privacy Act, which, while not as expansive as GDPR, contains similar provisions. The law, which goes into effect in January 2020, gives consumers the right to be informed regarding what information has been collected about them, rights to data access and portability, and the right to have their personal information deleted.[4] The law also expands the definition of personal information to include biometric data, location, and browsing history.[5] The state of Washington is currently working on similar legislation.[6]

There has also been a push to do more at the federal level in order to create, in the words of the U.S Chamber of Commerce, a "federal privacy framework that preempts state law on matters concerning data privacy in order to provide certainty and consistency to consumers and businesses alike."[7] Mr. Nemmers described the building momentum for legislation in Congress: *"This has gotten a lot of attention in DC. Lots of [congressional] committees are trying to get in on this. It's not a core topic that they're comfortable with, but they're moving forward ASAP because 20 states have proposed legislation."* He noted that a bill might include such elements as national preemption; applicability in all sectors; opt out by default but with the ability to opt in; a minimum standard of care for security; and breach notification.

Ethical and reputational challenges

On top of the constraints imposed by regulations, companies face the less explicit, but still significant, limitations associated with consumer sensitivities and public perceptions. Even if a certain use of data complies with regulatory requirements, customers and the broader public might still view it unfavorably. New and innovative uses of data may be particularly vulnerable to adverse reactions from the public, because they are more likely to be unfamiliar or violate traditional norms. But an important aspect of this issue is that consumer sentiment is unpredictable; companies lack certainty about what might spark a backlash. Familiar uses of data that have been tolerated before might suddenly face a change of opinion, while new uses that initially face resistance may become more acceptable as they demonstrate their utility.

Several ACLN members mentioned this concern. *"The data will be used in analytics and marketing. How far can you go without offending your customers and the public?"* one member asked. Another said, *"You don't want to do creepy things, because that's bad for the brand."* Members brought up emerging technologies and their potential to exacerbate the issue. *"The Internet of Things is going to bring a lot of these questions to both the commercial*

and consumer end of things. It's a different dimension, both in terms of the monetization and the risk. I think these things have yet to play out, but they will play out," a member noted.

Consumers remain skeptical about how companies are using data. In an April 2018 survey of consumers, only 20% of respondents said they fully trust companies to maintain their privacy. At the same time, 78% said that a company's ability to protect their data was extremely important, and 75% said they would not buy a product, no matter how good, from a company if they didn't trust the company to protect their data.[8] At the meeting, Mr. Jang summed up the challenge: *"Customers have high expectations in this area. The onus is on every company to provide transparency, process data fairly, and be accountable."*

The guests also noted that privacy is about more than consumer data, so it is an important issue for B2B as well as B2C companies. Human resources departments typically have a great deal of personal data, and data on business customers and suppliers may include personal data. There are also companies that sell data collection or analysis capabilities to other companies—embedded in products, for example. These companies may think that, since they are not the ones using the data, they are not responsible. The subjects of the data collected or analyzed, however, may see them as accomplices.

The response from companies

The overall challenge for companies is to ensure a proper balance between pursuing the opportunities presented by data and protecting the privacy of personal data. Regulations and norms must be respected, but the use of data in fruitful and innovative ways should not be restricted more than is necessary. With this imperative as a backdrop, members and guests discussed three major issues:

- Organizing the privacy function
- Obtaining adequate consent for the use of personal data
- Disclosing privacy incidents appropriately

Organizing the privacy function

Leveraging data while respecting privacy requires a sophisticated, centralized effort that draws upon a range of functions inside the company. Just as the GDPR requires a data protection officer for certain companies, members and guests noted that centralized leadership on privacy is key. *"Having someone looking out for all this is incredibly important. If it's across different groups, you could have disparate policies,"* a member said. At the meeting, Mr. Moore agreed: *"How do you get everyone on the same message? Start with the values of the company, then set out principles, then create a policy."* High-level decision-making is essential, he added: *"If you push authority too far down in the organization, you run a big risk. You need risks to be properly discussed at a high level of the organization."*

A company's leader on privacy—and where he or she fits into the organizational hierarchy—varies from company to company. Some companies have appointed chief privacy officers (CPOs) reporting to the CEO, and some experts see this as a growing (and beneficial) trend, giving the CPO the authority necessary to succeed.[9] In many companies, however, the person responsible for privacy issues is another executive, often from the legal or compliance function. It may even be the chief financial officer (CFO). One member noted that, at his company, the CFO is the lead on GDPR compliance, working with the head of IT on this issue.

Regardless of who leads the effort, however, centralized leadership needs to be supported by robust and coordinated activity further down in the organization. A member noted: *"Many big companies are siloed. Those units might do an outstanding job, but shouldn't they come together somewhere other than the top of the house? When we focus on compliance, we have a hierarchy. The CFO, GC, VPs, corporate audit folks, the legal group, IT all get involved. They meet on a regular cycle to talk about what's going on."*

One member had asked management to review how the company managed data across its many divisions and functions, and that effort led to a new approach at the company: *"They came up with a solution—a data council co-chaired by the person in charge of cyber and one of the attorneys in legal. It includes representatives from around the company. It has the purpose of getting hold of the data, where it is, how we're protecting it. So, we're taking it seriously—creating a focal point and a process for addressing it."*

The member noted the importance of including all business units, which are the first line of defense: *"The council is made up of business unit managers. The council has representatives from the whole range of business units that actually deal with data, so it can create a consistent approach."* Another member also highlighted the importance of the first line of defense: *"Privacy has to be integrated in overall business decisions. There are other people brought into that, including the GC's office, but ultimately, it's a business [line] owner's responsibility."*

The integration of privacy should not be an afterthought addressed late in the product development process, the guests explained. Having to bolt it on as the process is completed may be awkward and ineffective. Mr. Jang explained that privacy is now being considered earlier in product design: *"Lawyers are finally getting into engineering. We are doing privacy by design, which means considering the privacy impact of the features and functionality of a new product. There is often tension, lots of options and choices—judgment and a balancing of interests are required."*

What is the relationship between privacy and security?

There is a common perception that privacy and security are essentially the same thing, and that they are handled by the same corporate function. They are certainly related, because security is necessary to protect privacy, and the two functions should coordinate their efforts. Mr. Moore noted: *"I have a close relationship with the chief security officer … If I don't stay attached to security, I can't do what we promise."*

Yet the two concepts are distinct. Privacy goes beyond security, because it also depends on what a company intentionally does with personal data. Moreover, security goes beyond privacy, because security can be about data other than personal data (like product specifications). Mr. Andrade explained, *"The first step is to make sure we are secure. Then we make sure that data moves within that secure environment in a way that ensures privacy."*

Obtaining adequate consent for the use of personal data

Another important issue is obtaining consent for the use of personal data. Members and guests noted that communications with customers may need to go beyond the disclosures required by regulations. As a member explained in a pre-meeting conversation, *"The critical considerations are transparency and focus on the customer and end user. It's dynamic and will change over time, and we need to regroup and touch base. But if you're transparent and close to customers and end users, that will solve the vast majority of problems."* Another member added, *"You have to understand what's important to them, and if you're using their information, they have to know. Don't use a 92-page user agreement."*

Mr. Andrade said that well-formulated consent policies help minimize risk: *"It used to be that we could rely on implied consent. Now consent needs to be express and informed. It can't be buried. It has to be easy for a fifth grader to understand."* Members and guests acknowledged that customers don't always read the policies, but Mr. Moore added: *"Customers like the idea of control. Even if they don't exercise it, they like to know they have it."*

One member brought up an important factor in determining how willing customers are to accept that their data is being collected and analyzed: *"If people are getting value in return, they don't have concerns with privacy."* Surveys support this observation: When asked what would encourage them to share their data, respondents in a 2018 survey said that trust was the most important factor, followed by opportunities to receive free services or special offers.[10]

Disclosing privacy incidents appropriately

New requirements have caused companies to consider their policies for disclosing incidents in which the privacy of personal data has been violated in some way. Such a violation can stem

from a security breach in which an attacker has achieved access to personal data. However, it can also involve the intentional sharing of data by the company with other parties, or even the aggregation and analysis of data in a way that allows the company to infer new personal information about someone. Disclosures about security breaches are typically required by privacy-related regulations, while voluntary sharing of data is often regulated by requirements around consent.

The guests discussed some of the notification challenges under GDPR, which requires that a company notify the relevant regulator within 72 hours of becoming aware of a personal data breach that is likely to result in a risk to the "rights and freedoms" of the individuals involved.[11] Since "awareness" of a breach can be a matter of degree, it can be difficult to determine when the clock starts, the guests said. They also suggested that there may be uncertainty regarding the threshold for reporting, leading to frequent notifications. *"Tens of thousands of incidents have been reported to the regulators since GDPR, but the vast majority of them did not pose any real risk. There's a bit of notification fatigue now,"* Mr. Jang noted.

The guests advocated advance preparation for the various situations that might require disclosures, which they saw as inevitable. *"There are dry runs, exercises that are run on a routine basis. Every company will be different, but you have to exercise your muscles. We've advocated for elevated management and board participation,"* Mr. Nemmers explained. Mr. Andrade agreed, saying, *"You need a practiced, tight incident response plan. They're nuanced events. What you know in the first 12 to 48 hours is often wrong. It keeps changing. You need a well-practiced group that has good leadership and PR skills. You should have good privacy lawyers who can advise the company on when something has tripped the requirement of a public filing. It's a 'when' question, not an 'if' question."*

Board oversight

Boards face a familiar dilemma when trying to understand and assess their companies' efforts on privacy: navigating a complex issue with limited time and resources. They must decide which committees will be involved and what interactions and deliberations are necessary. As the guests noted, these issues are faced by all boards, not just those of consumer-facing companies.

Committees involved

While the full board is ultimately responsible, several committees are likely to be involved in overseeing privacy. The audit committee does not necessarily take the lead, though it often does, ACLN members noted. *"The audit committee handles it on the board, but the full board discusses it as well,"* one member said. *"The audit committee and the compliance and risk committee come together to talk about this,"* another added, explaining that *"there is an overlap with cybersecurity and privacy. If you put those committees together, it's almost the*

full board. When we cover those topics, we do it in combined fashion. We invite both committees. We want to be open and make sure everyone's comfortable."

At the meeting, a member mentioned another angle on committee involvement: *"The public policy committee is a place where you want to have attention paid as well. We could really mess up the US economy if we outlaw a lot of advertising and use of data. We could go way too far if we're not doing this right. The public policy committee or its equivalent should be preserving innovation and competition while attending to these issues."*

Board practices

The frequency and intensity of discussions about privacy still vary among boards. At some boards, discussions are regular and frequent. *"Privacy is reported on at every audit committee meeting,"* one member said. Another agreed, *"I suspect we talk about it in some form at every board and committee meeting."* In-depth discussions might take place at longer intervals: *"Once a year, we put these things together. We ask about the work of management. We have a regular agenda and then we have a focus on special topics—deep dives."*

Yet some boards are just getting started, especially when it comes to discussions about using data in new and innovative ways that might have privacy implications. These discussions are sometimes more ad hoc and dependent on management's initiative. One member said, *"To be honest, there are not a lot of conversations about this issue. There are some conversations when certain products are presented, but it's tangential, not a robust, specific discussion. We've had presentations on analytical stuff."*

The guests brought up additional considerations at the meeting. Mr. Andrade mentioned the role of internal audit in informing the board about the control framework for privacy: *"You need to have a control framework, so engage the internal audit folks … they have a rigor that a lot of lawyers don't have."* Mr. Moore brought up the challenge of hiring the right resources for the privacy function: *"One thing for the board to consider: compliance lawyers and privacy lawyers are almost impossible to hire—anyone trying to find privacy resources is finding them scarce. Make sure you have the right retention and compensation mechanism."*

Questions for boards to ask management about privacy

The meeting guests suggested several questions that boards should ask management about company privacy policies and practices:

- ? Has the company developed a coherent set of privacy principles?
- ? Is the privacy policy consistent with those principles?
- ? Is the policy easy to read and understand?
- ? Are business practices consistent with the policy?

Questions for boards to ask management about privacy

? Has there been a data-mapping exercise?

? Has there been an impact assessment?

? What is the internal control framework? What kind of assurance is applied?

? How does the company ensure privacy by design, and document that it does so?

Conclusion

As companies rush to take advantage of the data they are collecting from customers, employees, and others, they should pay close attention to both legal and reputational constraints on the use of personal data. ACLN members and their expert guests agreed that companies should address the issue of privacy at all levels of the organization, with business units working alongside centralized privacy leadership to implement policies and practices. Clear consent policies are important, as is careful preparation for the inevitable incidents that will require disclosures. Boards, in turn, have an opportunity to step up their oversight of privacy issues by discussing the issue frequently with management and by leveraging internal audit to understand the control framework around privacy. The issue goes beyond regulatory compliance; as one guest put it, *"if you haven't earned the trust of the customers, nothing else matters."*

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc. and EY and the associated logos are trademarks of EYGM Ltd.

US SCORE no. 06359-191US_2

Appendix 1: Guest biographies

Eduardo Andrade joined Booking Holdings (formerly known as the Priceline Group) in 2005 and serves as the global compliance and ethics officer. He is responsible for oversight and implementation of compliance and ethics programs across the company's six operating brands. Mr. Andrade also serves as associate general counsel, focusing primarily on data privacy.

Prior to joining Booking Holdings, Mr. Andrade practiced corporate law at Paul Hastings Janofsky & Walker in Stamford, Connecticut, and at Winston & Strawn in New York City. Prior to studying law, Mr. Andrade worked in the film industry and served as Harrison Ford's stand-in for *Patriot Games*, *The Fugitive,* and *Clear & Present Danger*.

Mr. Andrade also serves on the board of Guiding Eyes for the Blind, a not-for-profit guide dog school in Yorktown Heights, New York. He also is a former member of the Board of Fellows of Trinity College (Connecticut) and was a past president of the Westport Public Library Board of Trustees.

Mr. Andrade received a Bachelor of Arts from Trinity College (CT), a JD/MBA from Georgetown University, and is admitted to the New York and Connecticut bars. He is a Society of Corporate Compliance and Ethics Certified Compliance & Ethics Professional. In addition, Mr. Andrade is a Certified Information Privacy Professional through the International Association of Privacy Professionals.

Harvey Jang is senior director, global data protection & privacy counsel, and Asia Pacific, Japan, and China data protection & privacy officer for Cisco. He serves as the team lead for privacy and data security-related legal matters and is responsible for developing and orchestrating Cisco's global data protection policies, compliance capabilities, certifications, and accountability frameworks. Mr. Jang also has primary responsibility for privacy strategy in the APJC region for Cisco.

Prior to joining Cisco, Mr. Jang was senior director, legal affairs, for McAfee, part of Intel Security, where he was lead counsel for privacy, security, marketing, and antitrust compliance. In this role, he worked closely with engineers and product teams to develop and implement data protection policies and practices, design privacy-enhancing products and functionality, and manage legal compliance. Before McAfee, Mr. Jang was director of privacy and information management and chief privacy and security counsel for HP; senior compliance counsel for Symantec; and litigation counsel with O'Melveny & Myers.

He is a member of the board of trustees for Bowman School in Palo Alto, serves as an instructor for the International Association of Privacy Professional privacy credentials programs (CIPP/US, CIPP/Europe, and CIP/Technologist), and is a frequent panelist/speaker on a variety of topics related to privacy, security, and information governance.

Mr. Jang earned his Bachelor of Arts, magna cum laude, from UCLA and his JD, cum laude, from UC Hastings College of the Law. He is also a Fellow of Information Privacy (International Association of Privacy Professionals), Certified Information Security Manager (Information Systems Audit and Control Association), and Certified Information Professional (Association for Intelligent Information Management).

Tom Moore is chief privacy officer at AT&T. In this role, Mr. Moore oversees and verifies compliance programs for WarnerMedia and AT&T advertising and analytics. He works across AT&T's various operating companies to help set policies that align with the AT&T vision and establish "privacy by design" principles in the rollout of new products and services. His team's focus is to ensure the privacy of AT&T's customers and employees, and to safeguard important and confidential information.

In his previous role as senior vice president, human resources, Mr. Moore was responsible for the design, administration, and support of all executive compensation and management compensation and benefits plans for AT&T. He also oversaw human resources policy, which includes discount programs, HR technology systems, and international human resources functions, such as staffing, service delivery, and country management.

Mr. Moore has led diverse teams across finance, HR, and strategy, including as vice president of business development in the Corporate Strategy organization.

Before that, Mr. Moore was vice president and CFO of AT&T Advertising Solutions and Yellowpages.com, where he oversaw the sale of the business to Cerberus Capital Management.

Mr. Moore started his AT&T career in 1990 with Southwestern Bell Yellow Pages in St. Louis as an accounting supervisor; he held various finance positions, including business unit CFO and merger/integration controller. He is also an alumnus of EY.

Mr. Moore graduated cum laude with a bachelor's degree in Accounting from Xavier University in Cincinnati, where he also played varsity soccer.

He serves on the board of the AT&T Performing Arts Center and is a member of the American Institute of Certified Public Accountants. He also serves on the National Advisory Board of AT&T's HACEMOS employee resource group.

Phil Nemmers is a partner in Ernst & Young's cybersecurity practice with more than 30 years of experience supporting clients across various sectors, including financial services, health care, telecommunications, retail, consumer products, and aerospace and defense.

He is responsible for overseeing the firm's compliance and regulatory-related activities impacted by cybersecurity risk, and supporting the Office of Public Policy, Center for Board Matters, and Professional Practice Group on cybersecurity-related matters. This includes overseeing the firm's privacy vertical within its cybersecurity practice; leading Ernst & Young LLP's cybersecurity outreach activities with various federal regulators across key sectors and

the legislative branch; leading board insight sessions on cybersecurity risk management at numerous leading clients around the Americas; and evaluating the growing impact of cybersecurity risks on financial audits, internal audit activities, and third-party attestation activities.

Mr. Nemmers is a certified public accountant, a Certified Information Systems Auditor, and a Certified Information Technology Professional.

Appendix 2: Participants

Members participating in all or part of the meeting were:

- Ron Allen, Coca-Cola
- Sam DiPiazza, AT&T
- Bill Easter, Delta Air Lines
- Sheila Fraser, Manulife
- Charles Holley, Amgen
- Marie Knowles, McKesson
- Ellen Kullman, Dell Technologies
- John Mulligan, McDonald's
- Chuck Noski, Microsoft and Booking Holdings
- Tom Schoewe, General Motors
- Gerald Smith, Eaton
- Jim Turley, Citigroup and Emerson Electric
- John Veihmeyer, Ford
- David Vitale, United Continental
- Maggie Wilderotter, Hewlett Packard Enterprise

European Audit Committee Leadership (EACLN) members participating in all or part of the meeting were:

- Dagmar Kollmann, Deutsche Telekom
- Helman le Pas de Sécheval, Bouygues

Ernst & Young LLP was represented in all or part of the meeting by the following:

- Kelly Grier, US Chair and Americas Managing Partner
- John King, Americas Vice-Chair-Elect, Assurances Services
- Frank Mahoney, Americas Vice-Chair, Assurances Services

Appendix 3: Discussion questions for audit committees

? What new and emerging privacy regulations is your board most worried about?

? What kind of reputational issues related to privacy have come up as concerns of your board?

? What kind of efforts are underway at your company to assess and comply with privacy regulations? What kind of challenges are emerging?

? How is your company thinking about issues of trust and reputation as it develops new ways of using the data at its disposal?

? Which committee of the board takes the lead on privacy? How do other committees and the full board get involved?

? What kind of practices do you use to oversee privacy? Who comes to the board and how often is the issue discussed?

? Should boards be more proactive about addressing forward-looking privacy issues? How much should they rely on management to alert them to any issues?

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members in connection with the meeting.

[2] "GDPR Key Changes," EU GDPR Portal, accessed April 8, 2019.

[3] Ieuan Jolly, "Data Protection in the United States: Overview," Thomson Reuters Practical Law, October 1, 2018.

[4] Daisuke Wakabayashi, "California Passes Sweeping Law to Protect Online Privacy," *New York Times,* June 28, 2018.

[5] Dipayan Ghosh, "What You Need to Know about California's New Data Privacy Law," *Harvard Business Review,* July 11, 2018.

[6] Joseph O'Sullivan, "Washington Senate approves consumer-privacy bill to place restrictions on facial recognition," *Seattle Times,* March 6, 2019.

[7] U.S. Chamber of Commerce, "U.S. Chamber Releases Privacy Principles," news release, September 6, 2018.

[8] "IBM Survey Reveals Consumers Want Businesses to Do More to Actively Protect Their Data," The Harris Poll, accessed February 26, 2019.

[9] Doug Pollack, "Privacy is Taking its Place in the C-Suite," IDExperts, January 24, 2017.

[10] Foresight Factory, *Global Data Privacy: What the Consumer Really Thinks* (Conway, AK, and Sydney, Australia: Acxiom and the Global Alliance of Data-Driven Marketing Associations, May 2018), p. 15.

[11] "GDPR Key Changes," EU GDPR Portal, accessed April 8, 2019.